UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,401	07/12/2001	Thomas Robert Gruber	VIGN1840	5195

44654 7590 10/24/2006

SPRINKLE IP LAW GROUP
1301 W. 25TH STREET
SUITE 408
AUSTIN, TX 78705

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/905,401	GRUBER, THOMAS ROBERT	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-31 are pending in this office action, claims 30 and 31 are newly added.

2. Applicant's arguments, filed August 9, 2006, have been considered and are persuasive. However, a new ground of rejection is made.

Claim Objections

3. Claims 8 and 24 are objected to because of the following informalities: claim 8 ends in a comma instead of a period. Claim 24 should have "wherein said secure transaction is selected from" before the words "the group consisting of." Appropriate correction is required.

Claim Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 2 and 3 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claims 2 and 3 recites the limitation "token" and "authorization token," respectively. There is insufficient antecedent basis for this limitation in the claim. The proper recitation should be "transaction authorization token."

Claim Rejections - 35 USC § 103

8. Claims 1, 3-5, 7, 13, 14, 17, 22, 25, and 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Allen et al. (U.S. Patent Pub. No. 2002/0068629 A1) in view of Neuman et al. (Kerberos: An Authentication Service for Computer Networks, published September 1994).

Regarding claims 1 and 29, Allen et al. teaches a method of conducting a secure transaction with an on-line service while offline comprising the steps of:

- Preparing an off-line transaction object containing data to specify and request the secure transaction (all of fig. 5);
- Sending a message to the on-line service, said message containing the off-line transaction object (fig. 3 and fig. 6, ref. num 610); and
- Executing the off-line transaction object if the secure transaction is authorized (fig. 6, ref. num 614/618).

Allen et al. does not teach issuing a token to a user from an application server for the on-line service while the user is online with the online service and validating the transaction authorization token, where the validating is performed while the user is off-line from the service.

Neuman et al. teaches issuing a token to a user from an application server for the on-line service while the user is online with the online service (fig. 1, steps 1 and 2) and validating the transaction authorization token (fig. 1, steps 3 and 4), where the validating is performed while the user is off-line from the service (fig. 1, the user is offline from the ticket granting service during validation).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine issuing a token to a user from an application server while online with the service and validating a token, as taught by Neuman et al., with the method of Allen et al. It would have been obvious for such modifications because a token enables a user to login to a service for later use.

The combination of Allen et al. and Neuman et al. now suggests the message sent to the online service contains the off-line transaction object (fig. 5 of Allen et al.) and the transaction authorization token (fig. 1, steps 1 and 2 of Neuman et al.).

Regarding claim 3, the combination of Allen et al. in view of Neuman et al. teaches wherein the authorization token is issued to the user via a download operation while the user is on-line with the on-line service (see fig. 4, ref. num 426 of Allen et al.).

Regarding claim 4, the combination of Allen et al. in view of Neuman et al. teaches wherein the user prepares the off-line transaction object while the user is off-line from the on-line service (see paragraph 0043 of Allen et al.).

Regarding claim 5, the combination of Allen et al. in view of Neuman et al. teaches further comprising requesting a transaction authorization token, wherein the user requests the transaction authorization token for the secure transaction from the application server for the on-line service (see fig. 4, ref. num 424/426 and paragraph 0040 of Allen et al.).

Regarding claim 7, the combination of Allen et al. in view of Neuman et al. teaches wherein said issuing a transaction authorization token comprises generating a unique identifier when the token is issued, wherein said generating is performed by the on-line service (see fig. 3, ref. num 320 of Allen et al.).

Regarding claim 13, the combination of Allen et al. in view of Neuman et al. teaches wherein the transaction authorization token includes data representing a time

period during which the transaction authorization token is valid (see end of paragraph 0052 of Allen et al.).

Regarding claim 14, the combination of Allen et al. in view of Neuman et al. teaches wherein the transaction authorization token includes data representing a valid access duration for the transaction authorization token (see end of paragraph 0052 of Allen et al.).

Regarding claim 17, the combination of Allen et al. in view of Neuman et al. teaches further comprising encrypting the off-line transaction object (see paragraph 0040 of Allen et al.).

Regarding claim 22, the combination of Allen et al. in view of Neuman et al. teaches wherein the application server is a web-based application server (see paragraph 0019 of Allen et al.).

Regarding claim 25, the combination of Allen et al. in view of Neuman et al. teaches further comprising authenticating a user such that the user is online with the on-line service, wherein said authenticating is performed with a password and a network identity while the user is logging-on to the on-line service (see paragraph 0035 of Allen et al.).

Regarding claim 30, the combination of Allen et al. in view of Neuman et al. teaches wherein the transaction object includes an instruction to execute a function at the application server (see fig. 6, ref. num 618 of Allen et al.).

Regarding claim 31, the combination of Allen et al. in view of Neuman et al. teaches wherein the authorization token is a separate object from the off-line transaction object (see fig. 3 of Allen et al. and fig. 1 of Neuman et al.).

Claims 2, 6, 9-12, 15, 16, 19-21, 23, 24, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Allen et al. (USPGPUB '629) in view of Neuman et al. (Kerberos: An Authentication Service for Computer Networks, published September 1994), and further in view of Fischer (U.S. Patent Publication No. 2002/0010638 A1).

Regarding claim 2, Allen et al./Neuman et al. teaches all the limitations of claim 1, above. However, Allen et al./Neuman et al. does not teach wherein the token is issued to the user via an e-mail message sent from the application server for the on-line service.

Fischer teaches wherein the token is issued to the user via an e-mail message sent from the application server for the on-line service (paragraph 0025).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine issuing the token via an e-mail message sent from the application server, as taught by Fischer, with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because sending tokens via e-mail provides a user the credentials required for secure processing that can be saved and used at a later time. This is similar to a user signing up for a service (hotmail.com for example) and receiving an e-mail message with the login credentials in the e-mail message.

Regarding claim 9, the combination of Allen et al. in view of Neuman et al./Fischer teaches wherein the application server receives an incoming message including the transaction authorization token, checks the transaction authorization token for validity, and accepts or rejects the transaction authorization token (see fig. 6, ref. num 614 of Allen et al.).

Regarding claim 10, the combination of Allen et al. in view of Neuman et al./Fischer teaches wherein said sending a message to the on-line service containing the transaction authorization token and off-line transaction object comprises sending an e-mail message delivered to the application server via an asynchronous e-mail delivery method (see paragraph 0005 of Fischer).

Regarding claim 11, the combination of Allen et al. in view of Neuman et al./Fischer teaches where the asynchronous delivery mechanism is database record synchronization (see paragraph 0034 of Fischer).

Regarding claim 12, the combination of Allen et al. in view of Neuman et al./Fischer teaches where the asynchronous e-mail delivery method comprises a synchronization of data between a portable computing device and an on-line service (see paragraph 0022 of Fischer).

Regarding claim 21, the combination of Allen et al. in view of Neuman et al./Fischer teaches wherein the application server authorizes a specific transaction by a specific user on specific data objects such that the transaction authorization token can be used only once (see fig. 3, ref. num 318/320 and paragraph 0048 of Allen et al.).

Regarding claim 6, Allen et al./Neuman et al. teaches all the limitations of claims 1 and 5, above. However, Allen et al./Neuman et al. does not teach wherein the on-line service comprises the application server, and wherein the application server accesses a database.

Fischer teaches wherein the on-line service comprises the application server, and wherein the application server accesses a database (paragraph 0034).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine accessing a database, as taught by Fischer, with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because the database contains products to be ordered, by accessing the database, correct quantities can be obtained.

Regarding claim 15, Allen et al./Neuman et al. teaches all the limitations of claim 1, above. However, Allen et al./Neuman et al. does not teach wherein the transaction authorization token specifies an e-mail audit signature, and said transaction authorization token is valid only if the transaction is sent from an e-mail program via an e-mail delivery path that matches the e-mail audit signature.

Fischer teaches wherein the transaction authorization token specifies an e-mail audit signature, and said transaction authorization token is valid only if the transaction is sent from an e-mail program via an e-mail delivery path that matches the e-mail audit signature (paragraph 0025).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine an e-mail audit signature for verifying the token, as taught by Fischer, with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because the audit signature prevents intruders from

using a different e-mail address to trick the system into thinking the intruder is authorized.

Regarding claim 16, the combination of Allen et al. in view of Neuman et al./Fischer teaches wherein an e-mail address to which the message is sent varies according to an authorized data object and transaction type (see paragraph 0025 of Fischer).

Regarding claim 19, Allen et al./Neuman et al. teaches all the limitations of claim 1, above. However, Allen et al./Neuman et al. does not teach wherein the transaction authorization token is contained in a body or a header of an e-mail message.

Fischer teaches wherein the transaction authorization token is contained in a body or a header of an e-mail message (paragraph 0025).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the token contained in a body or header of an e-mail message, as taught by Fischer, with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because containing the token in the body of an e-mail message provides further authentication and authorization (see paragraph 0025 of Fischer).

Regarding claim 20, Allen et al./Neuman et al. teaches all the limitations of claim 1, above. However, Allen et al./Neuman et al. does not teach wherein the transaction authorization token and the off-line transaction object are attachments to an e-mail message.

Fischer teaches wherein the transaction authorization token and the off-line transaction object are attachments to an e-mail message (paragraph 0025).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the token and transaction object are attachments to an e-mail message, as taught by Fischer, with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because containing the token as an attachment of an e-mail message provides further authentication and authorization (see paragraph 0025 of Fischer).

Regarding claim 23, Allen et al./Neuman et al. teaches all the limitations of claim 1, above. However, Allen et al./Neuman et al. does not teach wherein said secure transaction is selected from the group consisting of a database modification, update, adding a file, and editing a file.

Fischer teaches wherein said secure transaction is selected from the group consisting of a database modification, update, adding a file, and editing a file (paragraph 0022).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine transactions consisting of modifications, updating, adding a file, and editing a file, as taught by Fischer, with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because editing a file allows the user to obtain the exact purchase order desired by the user.

Regarding claim 24, the combination of Allen et al. in view of Neuman et al./Fischer teaches the group consisting of a database modification, update, adding a file, editing a file, checking out a file, editing the file off-line, and checking in the file as an e-mail attachment (see fig. 4, ref. num 64/66/68 of Fischer).

Regarding claim 26, Allen et al./Neuman et al. teaches all the limitations of claim 1, above. However, Allen et al./Neuman et al. does not teach wherein the user comprises a software agent adapted to conduct the transaction on behalf of the user.

Fischer teaches wherein the user comprises a software agent adapted to conduct the transaction on behalf of the user (paragraph 0020).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a software agent that conducts transactions on behalf of the user, as taught by Fischer, with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because a software agent provides an automated process for the user to order products from a vendor.

Regarding claim 27, Allen et al./Neuman et al. teaches all the limitations of claim 1, above. However, Allen et al./Neuman et al. does not teach wherein the user sends the message to the on-line service while the user is offline from the online service.

Fischer teaches wherein the user sends the message to the on-line service while the user is offline from the online service (paragraph 0019).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine sending the message to the service while the user is offline from the online service, as taught by Fischer, with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because the user can provide the message ahead of time without having to log in to the service (see paragraph 0019 of Fischer). This saves time for the user by having the message already provided to the on-line service.

Regarding claim 28, the combination of Allen et al. in view of Neuman et al./Fischer teaches wherein the message to the on-line service is sent via e-mail (see paragraph 0025 of Fischer).

Claims 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Allen et al. (USPGPUB '629) in view of Neuman et al. (Kerberos: An Authentication Service for Computer Networks, published September 1994), and further in view of Konheim et al. (U.S. Patent No. 4,393,269).

Regarding claim 8, Allen et al./Neuman et al. teaches all the limitations of claim 1, above. However, Allen et al./Neuman et al. does not teach wherein the transaction authorization token is a one-way encryption of at least one of an identity of the user, a transaction type, and a data object for which the transaction is authorized.

Konheim et al. teaches wherein the transaction authorization token is a one-way encryption of at least one of an identity of the user, a transaction type, and a data object for which the transaction is authorized (col. 23, lines 52-62).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine an one-way encryption of the identity to create the token, as taught by Konheim et al., with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because the one-way encryption of the

identity provides a method for verifying both the content of the transaction and the parties involved (see abstract of Konheim et al.).

Regarding claim 18, Allen et al./Neuman et al. teaches all the limitations of claims 1 and 17, above. However, Allen et al./Neuman et al. does not teach wherein said encrypting comprises issuing a temporary public key that is a one-way encryption function of an address to which the secure transaction is to be sent for encryption of the off-line transaction object.

Konheim et al. teaches wherein said encrypting comprises issuing a temporary public key that is a one-way encryption function of an address to which the secure transaction is to be sent for encryption of the off-line transaction object (col. 23, lines 52-62).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine using an one-way encryption function for encrypting the transaction object, as taught by Konheim et al., with the method of Allen et al./Neuman et al. It would have been obvious for such modifications because the one-way encryption of the identity provides a method for verifying both the content of the transaction and the parties involved (see abstract of Konheim et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brad Hoff

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/17/06